# MARFORRES G-6

## SYSTEM AUTHORIZATION ACCESS REQUEST

## (SAAR) USER AND SUPERVISOR GUIDE

Service Desk Support 1-800-737-7034
(504) 697-7777

# Authorized SAARs and Certificates

MARADMIN 068/10:

- The only authorized SAAR form is the digital version of the DD2875 Dated Aug 2009. Any SAAR form dated prior to this date is NOT AUTHORIZED.
- The DD2875 form enables the use of digital signatures and is the only form that will be accepted.
- Hard Copies of SAARs WILL NOT be accepted. Digitally uploaded Hard Copies of SAARs WILL NOT be accepted.

# Authorized SAARs and Certificates

Per MARADMIN 118/11:

- The proper Cyber Awareness Training consists of
  1)"Careless Keystrokes Can Kill"
  2) Information Awareness Training Course
  3) Personally Identifiable Information Training Course

- As of 1 Jan 2012 the certificates listed above will need to be attached to any SAAR. If any of these documents are not attached the SAAR WILL NOT be processed.
- The only authorized way to take these courses is through MarineNet. Marine Net offers the necessary courses for Marines, Civilians and Contractors.
- AMHS SAARs are the ONLY SAARs that need the above certificates, as well as an Authorization Letter, and a CBT Certificate.

# IA Certificate

Official

United States Marine Corps

Completion Certificate

*This is to certify that*
JOE S. MARINE

*Has completed*
***DOD Information Assurance Awareness***
***Course Number: DODIA8***
*Given through the*
*Marine Corps Distance Learning Network*
*on Tuesday, August 24, 2010*

Semper Fidelis

T.K. Kerrigan
Colonel, U.S. Marine Corps
Director
College of Distance Education and Training

(Cert No.) 2914094

# PII CERTIFICATE

Official

United States Marine Corps

Completion Certificate

*This is to certify that*
Joe S. Marine

*Has completed*
*USMC Personally Identifiable Information (PII) Annual Training*
*Course Number: PII0090000*
*Given through the*
*Marine Corps Distance Learning Network*
*on Wednesday, December 14, 2011*

Semper Fidelis

T.K. Kerrigan
Director
College of Distance Education and Training

(Cert No.) 5414729

# CARELESS KEYSTROKES CAN KILL

Official

United States Marine Corps

MARINE CORPS COLLEGE OF DISTANCE EDUCATION AND TRAINING

Completion Certificate

*This is to certify that*

Joe S. Marine

*Has completed*

*Careless Keystrokes Can Kill*

*Course Number: CLKS01*

*Given through the*

*Marine Corps Distance Learning Network*

*on Wednesday, December 14, 2011*

Semper Fidelis

T.K. Kerrigan

Director

College of Distance Education and Training

(Cert No.) 5414781

# System Names

- **IT IS NO LONGER NECESSARY TO INCLUDE OTHER APPLICATIONS (I.E. CTS, MASTER PERSONNEL, TOP) IN THE SYSTEM NAME PORTION DUE TO THE FACT THAT THESE APPLICATIONS ARE ALL COVERED BY SHAREPOINT.**
- **If a user needs access to a site such as CTS or Master Personnel the user needs to request access to Sharepoint and then contact the owner of the site which they are requesting access to so they can be granted access to that site.**

# SAAR Header

- In the header on the SAAR form the user will ensure the type of request is selected (ie Initial request). Ensure that the DATE and LOCATION boxes are also completed. See below.
- The system name options are (as needed):
  - On a SAAR for Classified access: SIPR MCW, SIPR SharePoint, SIPR AMHS
  - On a SAAR for Unclassified access: NIPR SharePoint, NIPR AMHS

**SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)**

**PRIVACY ACT STATEMENT**

**AUTHORITY:** Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
**PRINCIPAL PURPOSE:** To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
**ROUTINE USES:** None.
**DISCLOSURE:** Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

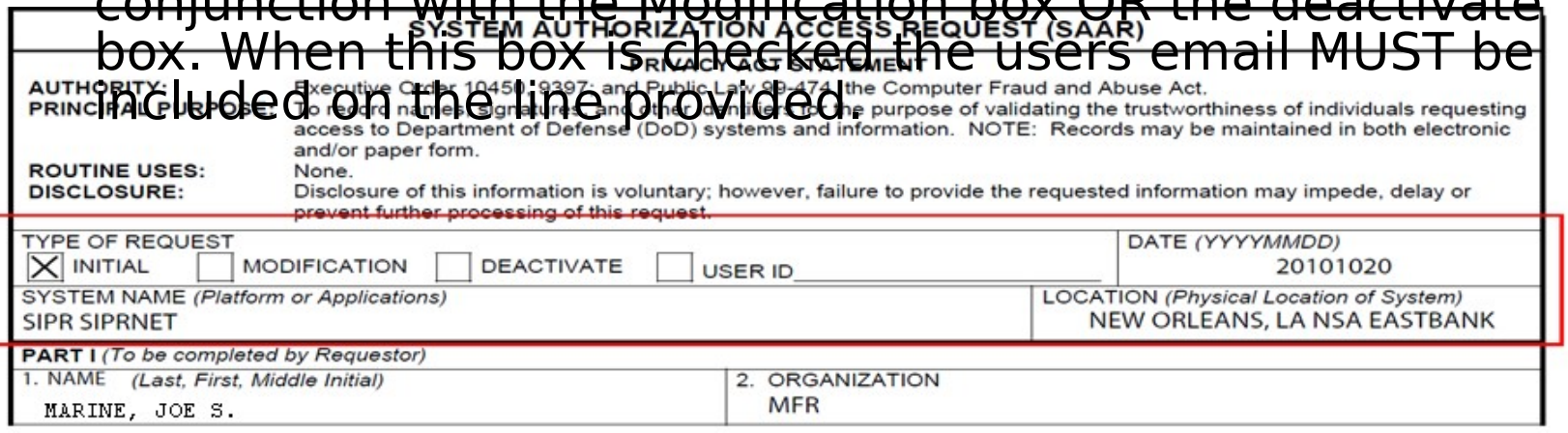
| TYPE OF REQUEST | DATE *(YYYYMMDD)* |
|---|---|
| [X] INITIAL [ ] MODIFICATION [ ] DEACTIVATE [ ] USER ID | 20101020 |
| SYSTEM NAME *(Platform or Applications)* SIPR MCW | LOCATION *(Physical Location of System)* NEW ORLEANS, LA NSA EASTBANK |

**PART I** *(To be completed by Requestor)*

| 1. NAME *(Last, First, Middle Initial)* | 2. ORGANIZATION |
|---|---|
| MARINE, JOE S. | MFR |

# Types of Requests

- **Initial**: First time requesting access to a certain application. Or if an application was deleted the initial box will be checked to have a new account created.
- **Modification**: Most commonly used for AMHS accounts. Only check this box if you are modifying an **<u>already existing</u>** account.
- **Deactivate**:  Only check if the SAAR is being submitted to have an already existing account deactivated.
- **User ID**: This box should only be checked in conjunction with the Modification box OR the deactivate box. When this box is checked the users email MUST be included on the line provided.



SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: [X] INITIAL [ ] MODIFICATION [ ] DEACTIVATE [ ] USER ID _____

DATE (YYYYMMDD): 20101020

SYSTEM NAME (Platform or Applications): SIPR SIPRNET

LOCATION (Physical Location of System): NEW ORLEANS, LA NSA EASTBANK

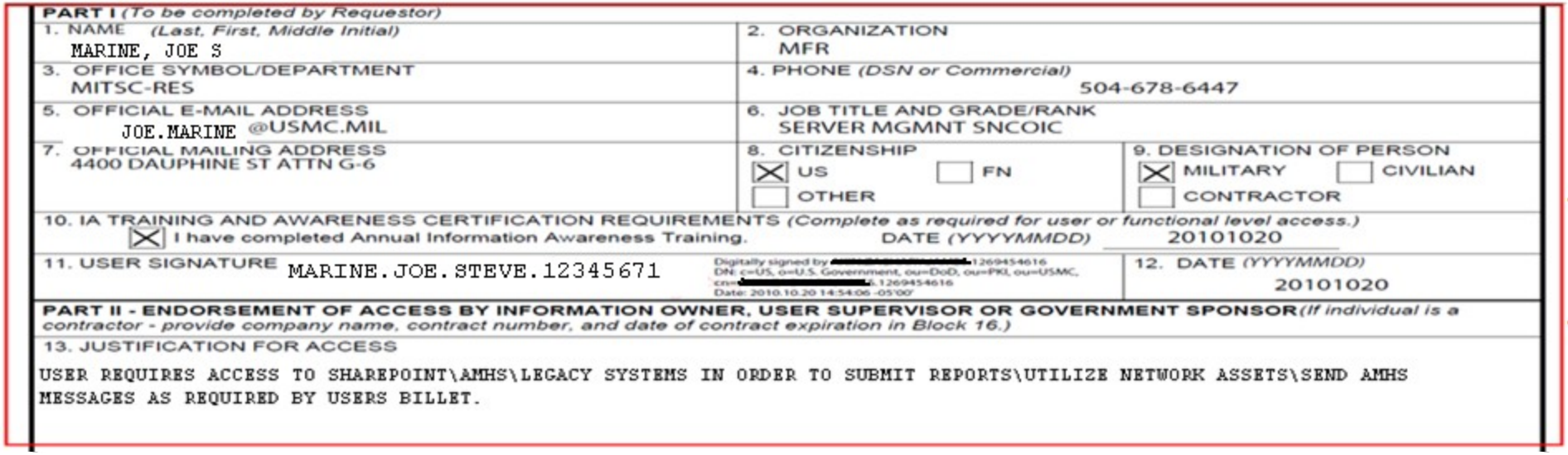
PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial): MARINE, JOE S.

2. ORGANIZATION: MFR

# Requestors Information

- Boxes 1 – 13 Box 26 must be completely filled out by the user. Additionally the Addendum pages (Last two Pages) Need to be initialed.
- If you do not currently have access to a computer to complete training requirements or electronically fill out your SAAR, speak with your ISC.
- Once the user has completed their portion of the SAAR (Blocks 1 – 13) AND the DOD required Cyber Awareness training they must email the both documents to their supervisor who will verify the request.
- Even if all of your required training is attached with the SAAR, box 10 must be filled out in its entirety. The date you completed your IA Training MUST be written in box 10.
- Box 12 is the date you are completing the SAAR.
- Box 11 needs to be the last box that gets filled out by the user. After that digital signature is placed on the SAAR it CAN NOT be changed.



**PART I** *(To be completed by Requestor)*

| | |
|---|---|
| 1. NAME *(Last, First, Middle Initial)*<br>MARINE, JOE S | 2. ORGANIZATION<br>MFR |
| 3. OFFICE SYMBOL/DEPARTMENT<br>MITSC-RES | 4. PHONE *(DSN or Commercial)*<br>504-678-6447 |
| 5. OFFICIAL E-MAIL ADDRESS<br>JOE.MARINE @USMC.MIL | 6. JOB TITLE AND GRADE/RANK<br>SERVER MGMNT SNCOIC |
| 7. OFFICIAL MAILING ADDRESS<br>4400 DAUPHINE ST ATTN G-6 | 8. CITIZENSHIP<br>[X] US [ ] FN<br>[ ] OTHER<br>9. DESIGNATION OF PERSON<br>[X] MILITARY [ ] CIVILIAN<br>[ ] CONTRACTOR |

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
[X] I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* 20101020

11. USER SIGNATURE MARINE.JOE.STEVE.12345671 Digitally signed by [redacted].1269454616 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=[redacted].1269454616 Date: 2010.10.20 14:54:06 -05'00'

12. DATE *(YYYYMMDD)* 20101020

**PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR** *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

USER REQUIRES ACCESS TO SHAREPOINT\AMHS\LEGACY SYSTEMS IN ORDER TO SUBMIT REPORTS\UTILIZE NETWORK ASSETS\SEND AMHS MESSAGES AS REQUIRED BY USERS BILLET.

# Pages 2-5

- Box 26- User Name: Must be filled out
- Box 27- Rules of Behavior: Must be completed
- Addendum Pages (Page 4-5)- Must both

26. NAME *(Last, First, Middle Initial)*
**Joe S. Marine**

27. OPTIONAL INFORMATION *(Additional information)*
By signing block 11 I agree to the following rules of behavior:
- I understand that I am providing both implied and expressed consent to allow authorized authorities, to include law enforcement personnel, access [redacted] which reside or were created on Government IT resources.
- I will not conduct any personal use that could intentionally cause congestion, delay, or disruption of service to any Marine Corps system or equipment.
- I will not install or use any Instant Messaging client or peer-to-peer file sharing application, except that which has been installed and configured to perform an authorized and official function.
- I will not use Marine Corps IT systems as a staging ground or platform to gain unauthorized access to other systems.
- I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the subject matter.
- I will not use Government IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- I will not use Government IT resources for personal or commercial gain without commander approval. These activities include solicitation of business services or sale of personal property.
- I will not create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials.
- I will not use Marine Corps IT systems to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity.
- I will not post Marine Corps information to external newsgroups, bulletin boards or other public forums without proper authorization. This includes any use that could create the perception that the communication was made in ones official capacity as a Marine Corps member, unless appropriate approval has been obtained or uses at odds with the Marine Corps mission or positions.
- I will not use Marine Corps IT resources for the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
- I will not modify or attempt to disable any anti-virus program running on a Marine Corps IT system without proper authority.
- I will not connect any personally owned computer or computing system to a DoD network without prior proper written approval.

27. Optional Information.

**PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION**

| 28. TYPE OF INVESTIGATION | | 28a. DATE OF INVESTIGATION *(YYYYMMDD)* | |
|---|---|---|---|
| 28b. CLEARANCE LEVEL | | 28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III | |
| 29. VERIFIED BY *(Print name)* | 30. SECURITY MANAGER TELEPHONE NUMBER | 31. SECURITY MANAGER SIGNATURE | 32. DATE *(YYYYMMDD)* |

DD 2875 ADDENDUM
STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

• You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

• You consent to the following conditions:

o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

o At any time, the U.S. Government may inspect and seize data stored on this information system.

o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and

User Initials ama

data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies

- Whether any particular communication or data qualifies for the protection Of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicabe privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

User Initials ama

# Supervisors Information

- Once the supervisor receives the SAAR and certificates the supervisor must complete the following steps
  1) Validate the IA cert is current by the date on the certificate.
  2) Validate and ensure the SAAR is filled out correctly To include Boxes 14-20b.
  3) Boxes 14-16 are often skipped. Please ensure these are checked.

14. TYPE OF ACCESS REQUIRED:
☐ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER

16. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. ☐

16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*

17. SUPERVISOR'S NAME *(Print Name)*

18. SUPERVISOR'S SIGNATURE

19. DATE *(YYYYMMDD)*

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT

20a. SUPERVISOR'S E-MAIL ADDRESS

20b. PHONE NUMBER

# Uploading the SAAR

- At this point the SAAR is now ready for routing and verification. Any errors or discrepancies the user and/or supervisor will be notified by email and if necessary a phone call.
- Supervisors or unit ISCs should be the ONLY people submitting SAARs. G6 Service Desk Marines are not authorized to submit SAARs for users.
- Two things should be noted
  1) If the user info has to be corrected it will need to be resigned by the user and resigned AGAIN by the supervisor.
  2) The user is responsible for checking on the status of their SAAR. It should not sit for longer than a day at any level.
- If a request is denied due to clearance issues the user will have to resubmit a SAAR when said issues are resolved.

# SAAR Process

- The SAAR form process is as follows:

ISC/Supervisor submits SAAR > G6 Service Desk verifies SAAR and JPAS information > Security Manager Signs SAAR > IA Managers Sign SAAR > NOC reviews the SAAR and creates account or forwards to proper authority for account to be created.

# Why did my SAAR get denied?

- Lack of Certification
- Date in Box 10 is not within current calendar year (IA DATE)
- Box 16 is not checked (Verification of need to know)
- "N/A" not suitable in Clearance Box (Security)
- Different System Name than SAAR Ticket states
- Invalid Signature
- User input in IA Portion
- Box 15 checked improperly ( Classification)
- No official mailing address
- Supervisor information is blank
- Location box empty
- Combining NIPR w/ SIPR SAARs or AMHS w/ other SAARs.

# Why did my SAAR get denied?

- Box 14 is not checked. (Authorized or Privileged)
- Double Signatures (User signs Supervisor etc.)
- No Background Investigation
- Unauthorized Security Manager. Authorized list is in link below.

https://portal.marforres.usmc.mil/sites/mfr/hq/other/cmd/Security/Shared%20Documents/Authorized%20Security%20Managers.pdf

- ADDENDUM pages not initialed/ Not attached to SAAR.
- Hand signed and/or digitally and hand signed
- Scanned SAAR
- Official email is not an official email. (first.last@usmc.mil)
- Contractors sign as supervisors. Contractors are not hired as individuals. Company hires the person, we pay the contract.

# Digital Signatures

- SAARs should only be signed once by each individual.
- If a SAAR has been digitally signed and then edited it will invalidate all of the digital signatures.
- If a SAAR needs to be edited ALL signatures must be removed, the SAAR edited and then resigned again.

# Security

| Investigation | Possible |
|---|---|
| NICI | Favorable, Unfavorable |
| NACLC | None, No Determination, Specified security level (Secret, TS, Unclass), Revoked |
| SSBI | None, No Determination, Specified security level (Secret, TS, Unclass), Revoked |
| SBPR | None, No Determination, Specified security level (Secret, TS, Unclass), Revoked |
| Others | None, No Determination, Specified security level (Secret, TS, Unclass), Revoked |

**N/A IS NOT ACCEPTABLE AS A SECURITY CLEARANCE. MUST BE ONE OF THE OPTIONS LISTED ABOVE.**

# SAAR USER GUIDE
# End Notes

Supervisors are advised to check their users security clearances before they submit a SAAR. The following should be noted

1. A clearance is not necessary for Unclassified access but an investigation by the security manager is needed.
2. Security clearances can take months to finish. During that time a user should attempt to get an interim clearance if the access requested is critical.

- Users should ensure that they keep copies of SAARs and Certificates for their records.
- A scanned copy of a BTR or MCTFS record showing current IA training will suffice in the absence of IA certificate.
- For official email address do not use a Yahoo! Or Gmail or any other commercial account. If you do not have one put N\A (Block 6).
- For users requesting admin privileges follow these guidelines
  1. Ensure Block 14 is checked as privileged due to admin accounts possessing elevated privileges.
  2. Ensure that specific justification is given as to why privileged access is needed for mission accomplishment.

# Summary

- Authorized SAAR forms
- Necessary Certificates
- How to properly fill out Users Information.
- How to properly fill out Supervisors information.
- Who submits the SAARs
- The SAAR Process
- Levels of Security Clearance
- What causes SAARs to get denied

# Questions